



# The Risky Business of Surveillance

Lauren Chalaturnyk, Partner

Andrew Skeith, Associate

Reynolds Mirth Richards & Farmer LLP

**Outline**

-  Legislative framework
-  When can you surveil?
-  "Internal" surveillance issues
-  "External" surveillance issues
-  Dealing with *FOIP* requests for surveillance info

2



## Legislative Framework



### Legislative Framework

- *Freedom of Information and Protection of Privacy Act (FOIPPA)* → applies to “public bodies”.
  - Includes municipalities as defined in the *Municipal Government Act*
- Regulates the collection, use, and disclosure of “personal information”.

## Personal Information

- Personal information means “recorded information about an identifiable individual,” including:

Name, address, telephone number

Race, religious beliefs, political associations

Biometric information (e.g., fingerprints, blood type)

Other people’s opinions about the individual

Educational, financial, employment, or criminal history

5

## Collection of Information

- A public body can only collect personal information if:
  - the collection is authorized by law,
  - the collection is for the purpose of law enforcement, or
  - the information relates directly to and is necessary for an operating program or activity of the public body.
- Public bodies must generally collect personal information directly from the individual it is about.

6

## Use of Information

- A public body must use personal information in a “reasonable manner”.
- A public body may use personal information only:
  - for the purpose for which it was collected (unless the individual consents to a different use), and
  - to the extent necessary to enable the public body to carry out its *purpose*.

7

## Use of Information

*Municipal Government Act, s. 3:*

- 3** The purposes of a municipality are
- (a) to provide good government,
  - (a.1) to foster the well-being of the environment,
  - (a.2) to foster the economic development of the municipality,
  - (b) to provide services, facilities or other things that, in the opinion of council, are necessary or desirable for all or a part of the municipality,
  - (c) to develop and maintain safe and viable communities, and
  - (d) to work collaboratively with neighbouring municipalities to plan, deliver and fund intermunicipal services.

8

## Disclosure of Information

- A public body may disclose personal information only as permitted by the *FOIPPA*, including:
  - to comply with a *FOIP* request,
  - if the individual has consented to the disclosure,
  - for the purpose of enforcing a legal right,
  - to assist in an investigation by law enforcement,
  - for use in court or an administrative proceeding,
  - for the purpose of “managing or administering personnel” of the public body, or
  - if the information is available to the public.

9

**When Can You  
Surveil?**

---

# "Internal" Surveillance Issues

## "Internal" Surveillance Issues

- Public bodies generally surveil their employees for two main reasons:
  1. Performance monitoring
    - Keystroke logging
    - Recording calls
    - GPS tracking
  2. Preventing misconduct
    - Video surveillance

## **"Internal" Surveillance Issues**

- When deciding whether to surveil employees, consider:
  - Whether there are legitimate issues to address
  - The effectiveness of the surveillance for addressing it
  - The intrusiveness of the method of surveillance
  - Whether there are other, less intrusive means of achieving the same goal
  - Whether the employees have notice of the surveillance
  - Whether the benefits of surveillance outweigh the reduction in privacy

13

## **"External" Surveillance Issues**

---

## Information Retention

- Once a public body collects personal information:
  - It should be accessed on a “need to know” basis, and only for the purpose for which it was collected,
  - It should be maintained securely and accessed only by authorized persons,
  - It should be retained only for as long as is necessary to meet the purpose of the collection,
  - Persons safeguarding the information should be subject to rules, protocols, etc., and
  - Sensitive information should be maintained separately from more general information.

15

## Liability

- *McAllister v Calgary (City)*
  - In 2007, in the early hours of New Year’s Day, the plaintiff was injured in a lengthy assault on a pedestrian overpass connected to Calgary’s C-Train system.
  - Despite having surveillance cameras in place, the City of Calgary did not detect the assault in real-time.
  - The offenders were convicted of criminal charges, but the plaintiff sued the City for its failure to detect and respond to the assault in a timely manner.

16



## Liability

- *McAllister v Calgary (City)*
  - The trial judge found that the City owed the plaintiff a duty of care as an “occupier” of the overpass.
  - The duty of care did not require the City to ensure complete safety, but *did* require it to have reasonable systems in place to detect and respond to assaults.
  - The City’s surveillance system was inadequate in the circumstances – video of the assault was unclear and difficult for City employees to see on small display monitors that would rotate every 3–4 seconds.
  - **Held:** The City was liable for damages suffered by the plaintiff after a reasonable response time of 10 minutes.

17

## Liability

- *McAllister v Calgary (City)* – Takeaways
  - Failure to adequately monitor municipal properties that are open to the public could result in the municipality being liable for injuries that occur there.
  - The adequacy of a municipality’s surveillance systems depends on factors such as:
    - The likelihood of criminality in the area,
    - The number and placement of cameras,
    - The quality of the video and adequacy of the lighting,
    - The number and size of monitors, and
    - The number of personnel (a) observing the monitors, and (b) patrolling the area.

18

# Dealing with *FOIP* Requests for Surveillance Information

---

## Information Rights

- Generally speaking, a person has a right to access any “record” in the control of a public body.
- To obtain copies of a record, a person must make a request to the public body in writing.
- Public bodies must make “every reasonable effort” to respond to and assist applicants.
- Disclosure is subject to the payment of a fee.

## Records

- Under the *FOIPPA*, “record” means a “a record of information in any form,” which includes:

Notes, books, and documents (typed or handwritten)

Photographs, maps, and drawings

Audiovisual recordings

21

## Exceptions to Disclosure

A public body *must* refuse to disclose personal information in response to a *FOIP* request if:

1. It could reasonably be expected to harm the business interests of a third party,
2. The information was collected on a tax return or for the purpose of determining tax liability,
3. It would reveal Cabinet deliberations or recommendations submitted to Cabinet, or
4. It would be an unreasonable invasion of a third party’s personal privacy.

22

## Exceptions to Disclosure

A public body *may* refuse to disclose personal information in response to a *FOIP* request if it:

1. Could reasonably be expected to threaten someone's health or safety,
2. Was provided in confidence for the purpose of assessing suitability for employment,
3. Could reasonably be expected to harm law enforcement interests,
4. Could reasonably be expected to harm intergovernmental relations,

23

## Exceptions to Disclosure

5. Could reasonably be expected to reveal:
  - A draft of a resolution or bylaw that has not been considered in a public meeting, or
  - The substance of deliberations of a private meeting of the public body's elected officials.
6. Could reasonably be expected to reveal:
  - Advice, proposals, plans, or recommendations developed by or for a public body or Cabinet, or
  - Consultations or deliberations involving the employees of a public body or a member of Cabinet.

24

## Exceptions to Disclosure

7. Could reasonably be expected to harm the economic interests of a public body,
8. Relates to testing or auditing procedures or techniques,
9. Is subject to any type of legal privilege (including solicitor-client privilege),
10. Could reasonably be expected to harm a historic resource or any rare or endangered form of life, or
11. Is readily available to the public (or will be released within 60 days after the request).

25

## Exceptions to Disclosure

- If a requested record is in the control of another public body, the public body that received the request may transfer it to the other public body.
  - The time limit for transferring a request is 15 days after the request was received.
- If information excepted from disclosure can be severed from a record, an applicant has a right to access the remainder of the record.

26

## Third Party Intervention

- Before giving access to a record that may harm the economic interests or privacy of a third party, a public body must give them written notice.
- When a public body gives notice, it must wait until either the third party responds or 21 days elapses before it decides to disclose the record.
- If the public body discloses the record, it must give notice to the affected third party, who may then ask the OIPC to review the decision to disclose.

27

## Time Limit for Responding

- Public bodies must make every reasonable effort to respond to a request within 30 days.
- However, a public body may extend this deadline with permission from the OIPC if:
  - The applicant gives insufficient detail,
  - The applicant requests a large volume of records,
  - More time is needed to consult with a third party, or
  - To accommodate the rights of third parties.
- If the deadline is extended, the public body must inform the applicant.

28



Reynolds Mirth Richards & Farmer LLP  
1800 Stantec Tower, 10220 – 103 Avenue  
Edmonton AB Canada T5J 0K4  
P: 780.425.9510 F: 780.429.3044

Thank you for  
attending

1.800.661.7673 (RMRF)  
[www.rmrf.com](http://www.rmrf.com)

Lauren Chalaturnyk  
780.497.3352  
[lchalaturnyk@rmrf.com](mailto:lchalaturnyk@rmrf.com)

Andrew Skeith  
780.497.3377  
[askeith@rmrf.com](mailto:askeith@rmrf.com)